CLAIMS

1. A hybrid stream cipher operating within a computing device, comprising:

a first software routine to divide incoming plain text into variable-sized blocks; and

a second software routine to convert the plain text into cipher text based on an encryption key and an internal identifier.

2. The hybrid stream cipher of claim 1, wherein the first software routine produces the variable-sized blocks based on the encryption key, the internal identifier and an output of a first non-linear function.

3. The hybrid cipher of claim 2, wherein each current block of the plain text is determined by (i) producing a pseudo-random sequence using a second non-linear function including the encryption key, the internal identifier and the output of the first non-linear function as inputs and (ii) accessing contents of the pseudo-random sequence as a number of data elements of the plain text forming the current block.

4. The hybrid cipher of claim 1, wherein the second software routine further performs a first shuffling operation on an internal state of a computing device based on the encryption key so that a single bit modification of the encryption key requires complete recalculation of the internal state of the computing device.

5. The hybrid cipher of claim 4, wherein the second software routine further performs a second shuffling operation on the internal state of the computing device based on at least the internal identifier to mitigate a likelihood of prediction of the internal state of the computing device upon knowledge of the encryption key.

6. The hybrid cipher of claim 1 further comprising:

a third software routine to determine if a plurality of random data elements are to be distributed within the cipher text.

7. The hybrid cipher of claim 6, wherein the third software routine determines an amount of random data elements distributed within the cipher text is programmable based on a percentage value entered by a user, or set based on the encryption key and internal identifier and the internal state of the hybrid stream cipher.

8. The hybrid cipher of claim 6, wherein the third software routine determines an amount of random data elements distributed within the cipher text is set based on the encryption key, the internal identifier and the internal state of the computing device.

9. The hybrid cipher of claim 6, wherein the plurality of random data elements are produced by a pseudo-random generator.

10. The hybrid cipher of claim 1 further comprising a third software routine to map the input plain text before undergoing operations of the second software routine to avoid statistics of the plain text from reflecting an internal state of the computing device.

11. The hybrid cipher of claim 1 further comprising a third software routine to produce an output stream based on a mixing of the cipher text, a plurality of random data elements and a hash digest of a portion of the output stream.

12. The hybrid cipher of claim 1 further comprising a third software routine to distribute one of a digital signature and a watermark in the cipher text in order to detect modification.

13. The hybrid cipher of claim 12 further comprising a fourth software routine to calculate and distribute a hash of the cipher text, a plurality of the random data elements and the digital signature within an output stream.

14. The hybrid cipher of claim 1 further comprising a third software routine to convert cipher text to plain text based on a table lookup using an array having data elements that are permuted to correspond to an inverse of an array of an internal state of the computing device.

15. A computing device comprising:

a memory; and

logic to perform a stream cipher operation using an encryption key on input data segmented in random sized blocks.

16. The computing device of claim 15, wherein the stream cipher operation involves encryption.

17. The computing device of claim 15, wherein the logic is an integrated circuit.

18. The computing device of claim 15, wherein the hybrid stream cipher processed by the logic produces random-sized blocks of the input data based on an encryption key, the unique internal identifier and an output of a first non-linear function.

19. The computing device of claim 18, wherein each block of the plain text is determined by the hybrid stream cipher (i) producing a pseudo-random sequence using a second non-linear function including the encryption key, the internal identifier and the output of the first non-linear function as inputs and (ii) accessing contents of the pseudo-random sequence as a number of data elements of the plain text forming the current block.

20. The computing device of claim 15, wherein the computing device is a smart card.

21. The computing device of claim 15, wherein the computing device is a node coupled to a network and alternatively a router.

22. The computing device of claim 15, wherein the logic of the computing device is an operating system.

23. The computing device of claim 15, wherein the computing device is a wireless device.

24. The computing device of claim 15, wherein the memory of the computing device is a portable storage medium that, only when in communication with the logic, enables the logic to perform the stream cipher operation on the random-sized blocks.

25. A method for decrypting input data using a combination of stream cipher and block cipher functionality, comprising:

receiving as input a cipher text, a decryption key, a percentage of random data and a unique internal identifier; and

reiteratively decrypting blocks of the cipher text using the decryption key, the percentage of random data and the unique internal identifier to recover corresponding blocks of plain text.

26. The method of claim 25 further comprising verifying a digital signature distributed in the cipher text and aborting decryption if one bit of the plain text has been changed.

27. A mechanism for securely selling digital content, comprising:

assigning a unique internal identifier to each user;

receiving a request from a user for a download of the digital content;

encrypting the digital content using a hybrid stream cipher, the hybrid stream cipher using as inputs the internal identifier, an encryption key, and a percentage of random data value to control conversion of the digital content into an encrypted digital content; and

transmitting the encrypted digital content to the user.

28. The mechanism of claim 27 includes a copyright in one of a plain text form, an image or an icon to operate as a digital signature, that is needed for decrypting the digital content and allowing the digital content to be uniquely sold to a particular user.

29. The mechanism of claim 27, wherein the digital content is software that is placed on a removable media or downloaded on-line.